EL CORTAMEGOS HUMANO

WILBERT WUSYNTH

El Cortafuegos Humano

Una novela de Wilbert Wusynth

Por **Wilbert Wusynth**

Madrid, 2026

©WilbertWusynth

Elena Vega, analista del Centro de Operaciones de Seguridad del Banco Europeo Meridional en Madrid, detecta a las 3:47 de la madrugada un patrón anómalo: microtransferencias hacia Singapur que siguen una curva de escalamiento exponencial. El SIEM las clasifica como bajo riesgo, y su jefe, Marcos Durán, las descarta como ruido. Esa misma noche recibe un mensaje anónimo: *«Deja de mirar donde no debes.»*

Novela co-escrita con IA. Debate ético tras un libro creado con IA: ¿quién es el verdadero autor?

Wilbert Wusynth, coautor de novelas escritas con inteligencia artificial, asume sin disimulo su método de trabajo y lo defiende como una elección consciente de orquestación creativa.
Su método**:** se concibe como un director de cine, no como un guionista. La IA genera la prosa; él aporta juicio, estructura y voz, interviniendo solo cuando el resultado no lo convence. Escribe con sus propias manos alrededor del 10% del texto, sobre todo los diálogos.
Sus tesis principales:

- La categoría "100% escrito por IA" es hueca: ningún modelo genera hoy una novela autónoma de principio a fin sin dirección y edición humana. La IA es amplificador, no autora.
- Rechaza la presión de etiquetar obras por porcentaje de generación artificial. Lo considera imposible de medir y "un poco tonto"; recuerda que los escritores fantasma y los editores extensos tampoco se declaran.
- El debate sobre el oficio le interesa poco: lo que importa es la historia y su capacidad de conmover, no la genealogía de las palabras.
- Acepta que la resistencia de los autores consagrados es comprensible, pero la convivencia entre escritura tradicional y asistida

por IA es inevitable. "El genio ya está fuera de la botella".

- Critica el mal uso negligente de la IA —libros mal escritos por quien no sabe gestionar la herramienta—, no la herramienta en sí.
- Cierra con un matiz: aunque rechaza las declaraciones obligatorias, defiende la divulgación voluntaria, porque la transparencia contribuirá a normalizar el uso. La normalización, dice, vendrá del contacto y la conversación, no de las reglas.

Posición de fondo: ni apocalíptico ni entusiasta ciego. Partidario de la herramienta, crítico con su mal uso, escéptico ante los purismos y convencido de que la buena literatura se reconoce en la página, no en la huella dactilar de quien la tecleó.

El Cortafuegos Humano

Capítulo 1 — Pulso anómalo

La pantalla del SIEM bañaba la sala en una luz azulada que a Elena Vega siempre le recordaba a un acuario. Un acuario silencioso, frío, poblado de criaturas invisibles que nadaban contra corriente en la oscuridad de las redes.

Eran las 3:47 de la madrugada en el Centro de Operaciones de Seguridad del Banco Europeo Meridional, y Elena llevaba ya nueve horas sentada frente a su estación de trabajo. El SOC, un búnker de cristal y cableado en la planta cuarta de la torre corporativa de Madrid, estaba desierto salvo por ella y el zumbido constante de los ventiladores de los servidores que respiraban dos pisos más abajo, en el data center subterráneo.

Su café se había enfriado hacía rato. No importaba. Lo que importaba era la anomalía.

Había comenzado como un parpadeo insignificante en el dashboard de tráfico de red: una serie de microtransferencias, cada una inferior a los quinientos euros, dirigidas a cuentas bancarias en Singapur. Por sí sola, cada transacción era invisible para los filtros automáticos: demasiado pequeña para activar los umbrales de alerta del sistema antifraude, demasiado ordinaria para que el módulo de detección de anomalías la clasificara como sospechosa. Pero Elena no miraba las transacciones individuales. Miraba el patrón.

Catorce transferencias en seis horas, todas originadas desde el mismo segmento de red interno, todas dirigidas a cuatro cuentas distintas en Singapur, todas

ejecutadas en intervalos irregulares que seguían una curva de distribución que ella reconocía.
Era un reconocimiento. Alguien estaba probando el sistema, midiendo tiempos de respuesta, calculando ventanas de latencia. Era el tipo de comportamiento que precedía a un asalto mayor, la equivalencia digital de un ladrón que golpea las paredes buscando puntos débiles antes de perforar la caja fuerte.
El SIEM, sin embargo, no estaba de acuerdo. El sistema había clasificado la actividad como «bajo riesgo», asignándole una puntuación de treinta y siete sobre cien. Para el algoritmo, aquellas microtransferencias no eran más que ruido de fondo, el tráfico normal de un banco internacional que movía miles de millones cada día. Elena sabía que el algoritmo tenía razón en términos estadísticos. También sabía que los algoritmos no tienen instinto.
Abrió la consola de análisis de flujo de red y amplió el rango temporal. Las microtransferencias habían comenzado tres días antes, con una frecuencia de una cada doce horas. Ayer habían aumentado a dos por hora. Esta noche, cuatro en seis horas. La aceleración era exponencial, y la curva apuntaba a un punto de inflexión que, si proyectaba la tendencia, llegaría en algún momento del fin de semana.
Algo se estaba preparando. Algo grande.
Marcó la extensión interna de Marcos Durán, jefe de ciberseguridad. El teléfono sonó seis veces antes de que una voz ronca y adormilada respondiera.
—Dime.
—Marcos, soy Elena. Tenemos actividad anómala en el segmento de transferencias internacionales. Microtransacciones hacia Singapur, patrón de reconocimiento. Creo que alguien está sondeando el sistema SWIFT.

Un silencio. Luego, un suspiro que Elena conocía demasiado bien: ese sonido que significaba que Marcos iba a decir algo que ella no quería oír.

—¿Qué puntuación le da el SIEM?

—Treinta y siete.

—Treinta y siete, Elena. Eso es ruido blanco. Sabes cuántas alertas de bajo riesgo recibimos cada semana.

—Sé cómo funciona el SIEM. También sé que esta no es actividad normal. La distribución temporal sigue una curva de escalamiento. Si proyecto la tendencia...

—Llevas demasiadas noches sin dormir.

La frase aterrizó como un golpe seco. Elena cerró los ojos y contó hasta tres. No iba a servir de nada discutir con Marcos a las cuatro de la madrugada por teléfono. Nunca servía de nada discutir con Marcos, pensara lo que pensara.

—Solo pido que revises los logs cuando llegues. Si consideras que no hay nada, lo descartamos.

—Lo haré. Ahora vete a casa, Elena. En serio.

Colgó. Elena dejó el teléfono sobre la mesa y se quedó mirando la pantalla, donde una nueva microtransferencia acababa de aparecer en el dashboard: quinientos doce euros hacia una quinta cuenta en Singapur que no estaba en la lista anterior. El atacante estaba ampliando su mapa de destinos.

Actuó por instinto. Abrió la herramienta de captura de pantalla y documentó cada transacción, cada marca de tiempo, cada dirección IP de origen y destino. Guardó las capturas en una carpeta temporal y luego, después de un momento de duda, las copió a una unidad cifrada personal que llevaba siempre en el llavero. Era una violación técnica de protocolo: los datos de seguridad del banco debían permanecer dentro de los sistemas del banco. Pero Elena había aprendido, en sus doce años de carrera, que la evidencia tiene la

mala costumbre de desaparecer cuando alguien con suficientes privilegios quiere que desaparezca.
Cerró sesión, recogió sus cosas y recorrió el pasillo hasta el ascensor. El edificio entero estaba en silencio, iluminado por la luz de emergencia que dibujaba halos ámbar en las paredes de cristal. El ascensor la llevó al aparcamiento subterráneo, donde su coche esperaba solo entre dos filas de plazas vacías.
Cuando arrancó el motor, su móvil vibró en el bolsillo. Lo sacó pensando que era Marcos, quizás recapacitando.
No era Marcos.
Era un mensaje de un número desconocido, sin remitente, sin asunto. Seis palabras en la pantalla: *Deja de mirar donde no debes.*
Elena se quedó inmóvil, con el motor al ralentí y el aire acondicionado soplando sobre sus manos frías. Miró el mensaje una vez más, luego el espejo retrovisor, luego las sombras del aparcamiento. No había nadie.
Salió del garaje con una sensación que no era exactamente miedo, sino algo peor: la certeza de que alguien la estaba observando.

Capítulo 2 — El anzuelo perfecto

Tres años antes, Elena había vivido la peor semana de su carrera profesional. Un ejecutivo del área de fusiones y adquisiciones —homónimo del CEO, firma manuscrita en la intranet, acceso a documentos confidenciales— había recibido un correo que parecía enviado por el departamento de recursos humanos. Asunto: «Revisión de beneficios — Acción requerida». El correo le pedía que actualizara sus credenciales en un portal que replicaba con precisión milimétrica la página de acceso del banco. El ejecutivo introdujo su usuario y contraseña. Doce millones de euros

desaparecieron en una cadena de transferencias que cruzó cuatro países antes de volverse irrastreable.
El banco nunca recuperó el dinero. El ejecutivo dimitió. Y Elena, que por aquel entonces era analista junior en el equipo de conciencia de seguridad, decidió que nunca más volvería a confiar en la naturaleza humana como primera línea de defensa.
Desde entonces, ella diseñaba las simulaciones de phishing interno del banco. Cada trimestre, los empleados recibían correos trampa diseñados por Elena: algunos burdos, otros tan sofisticados que incluso los miembros del equipo de seguridad caían en ellos. Los que picaban recibían formación obligatoria. Los que reportaban los correos ganaban puntos en su evaluación de conciencia de seguridad. Era un sistema imperfecto, pero había reducido la tasa de clics del treinta y dos por ciento al seis por ciento en tres años.
Ahora, sentada en su apartamento de Chamberí con el mensaje anónimo aún en la pantalla del móvil, Elena pensaba en aquel ejecutivo de hace tres años. Se preguntaba cuántos anzuelos más habrían caído en el agua sin que nadie los hubiera visto.
A las ocho de la mañana llegó al SOC. El turno de día ya estaba activo: cuatro analistas en sus puestos, auriculares puestos, monitores parpadeando. Elena los saludó con un gesto y se dirigió a su estación. No había dormido, pero la adrenalina del mensaje anónimo la mantenía en un estado de alerta que el cansancio no podía penetrar.
Lo primero que hizo fue acceder a los logs de correo del servidor Exchange. Si el atacante había realizado reconocimiento sobre el sistema de transferencias, lo más probable era que hubiera intentado comprometer credenciales de empleados con acceso privilegiado. El phishing seguía siendo, a pesar de todos los avances técnicos, el vector de entrada más utilizado en ataques

dirigidos. No porque fuera sofisticado, sino porque funcionaba.

Filtró los logs por los últimos sesenta días, buscando correos que hubieran sido marcados por el sandbox de attachments como sospechosos pero no necesariamente maliciosos: documentos con macros, enlaces a dominios recién registrados, archivos ofimáticos con comportamiento anómalo. El sistema de filtrado automático era bueno, pero no perfecto. Los ataques dirigidos usaban técnicas de evasión que a menudo pasaban desapercibidas para los filtros heurísticos.

El resultado la heló.

Tres empleados de alto nivel habían abierto enlaces maliciosos en las últimas cuatro semanas. Los tres habían recibido correos que el sandbox había clasificado como «sospechoso pero no confirmado» y que, por una combinación de mala configuración de cuarentena y saturación de la cola de revisión manual, nunca habían sido escalados al equipo de respuesta. El primero era un director financiero. El segundo, la jefa de tesorería. El tercero era Marcos Durán.

Elena se quedó mirando la entrada en el log: un correo supuestamente enviado desde la dirección del proveedor de soluciones SIEM, con un enlace a un portal de «descarga de parches de seguridad». Marcos había hecho clic a las once de la noche de un martes, fuera de horario laboral, desde su portátil corporativo. El enlace había redirigido a una página de autenticación falsa que capturaba credenciales.

¿Marcos había sido víctima de phishing? ¿O había abierto aquel enlace a propósito, sabiendo que era una puerta trasera que él mismo había ayudado a instalar?

La pregunta era tan incómoda que Elena la apartó mentalmente, como quien cierra un cajón que contiene algo que no quiere ver.

Necesitaba más datos. Y necesitaba que alguien dentro de la red le revelara sus intenciones sin saber que estaba siendo observado.

Diseñó un honeypot: un correo falso que simularía ser una alerta de seguridad interna, dirigido a una lista reducida de empleados con acceso a sistemas críticos. El correo informaría de una supuesta brecha en el sistema de autenticación y pediría a los destinatarios que accedieran a un portal de verificación mediante un enlace. El portal, alojado en un servidor controlado por Elena, registraría la dirección IP de origen, las credenciales introducidas y el timestamp. Si alguien intentaba usar las credenciales capturadas, Elena lo sabría de inmediato.

Era, técnicamente, una operación de cebo. No estaba autorizada por ningún protocolo formal del banco. Si la descubrían, podía enfrentarse a un expediente disciplinario, o peor. Pero la alternativa era esperar a que el atacante diera su siguiente paso, y Elena había visto demasiadas veces cómo terminaba la espera: con un saldo en rojo y un ejecutivo dimitiendo.

Configuró el honeypot con cuidado. Usó un dominio recién registrado que imitaba el dominio interno del banco con una variación casi imperceptible: un carácter cirílico en lugar de un carácter latino, una técnica llamada homoglyph attack que los filtros antiphishing rara vez detectaban. Redactó el correo con el tono seco y técnico que usaba el equipo de seguridad en sus comunicaciones internas. Lo programó para enviarse a las diez de la mañana, cuando la mayoría de los destinatarios estaría en sus puestos y la urgencia de una alerta de seguridad parecería plausible.

A las diez y doce, el primer clic llegó. Elena observó cómo el portal de captura registraba la dirección IP: interna, corporativa, perteneciente al segmento de red

de la planta ejecutiva. Las credenciales introducidas pertenecían a un contable del departamento de tesorería. Diez minutos después, un segundo clic. Esta vez la IP era diferente: venía del segmento de red del área de tecnología.
A las once y media, un tercer clic. Este no venía de un empleado que hubiera recibido el correo, sino de alguien que había reenviado el enlace a otra dirección interna. Elena rastreó el reenvío: la cuenta origen pertenecía a un técnico de sistemas. La cuenta destino no existía en el directorio activo del banco.
Era una cuenta fantasma. Alguien dentro de la red había creado una identidad falsa, o había comprometido una cuenta inactiva, y la estaba usando para moverse lateralmente por el sistema.
El honeypot había mordido. Y el pez que había picado no nadaba en aguas externas: estaba dentro del acuario.

Capítulo 3 — Huellas en la memoria

Elena necesitaba ver el interior de la máquina comprometida. No los logs, no las métricas de red, no las alertas del SIEM: la memoria viva del equipo, el espacio efímero donde los procesos respiran antes de morir y donde los atacantes dejan huellas que solo existen mientras la máquina está encendida.
El problema era que el equipo en cuestión —el portátil de Marcos Durán— estaba asignado al segmento ejecutivo, y Elena no tenía privilegios de administrador sobre ese segmento. Su cuenta de analista le permitía monitorizar tráfico y revisar logs, pero no acceder a imágenes forenses de endpoints de alto nivel. Esa capacidad estaba reservada a los administradores de sistema, y el único administrador con acceso al

segmento ejecutivo era Iván Soler, su compañero del equipo de infraestructura.
Iván estaba en Tenerife, de vacaciones, con el móvil en modo avión y el correo en respuesta automática. Volvería en una semana.
Una semana era una eternidad. El atacante estaba dentro, moviéndose, y cada hora que pasaba era una hora que usaba para consolidar su posición o, peor, para borrar sus huellas. Elena lo sabía: los atacantes que operaban con paciencia y recursos no dejaban evidencia estática. Limpiaban logs, modificaban timestamps, inyectaban procesos legítimos para enmascarar los maliciosos. La única evidencia fiable era la que todavía flotaba en la memoria RAM, y la memoria RAM se borraba en el instante en que la máquina se apagara.
Elena sopesó sus opciones. Podía escalar formalmente a Dirección, solicitar privilegios de emergencia, esperar a que el comité de seguridad aprobara el acceso. Eso tomaría días, si es que llegaba a aprobarse, y mientras tanto Marcos —si era víctima o cómplice— seguía usando su portátil, generando nueva actividad que sobrescribiría los artefactos de memoria que Elena necesitaba analizar.
O podía saltarse el protocolo.
La decisión no fue fácil. Elena había construido su carrera sobre el respeto a las reglas. Doce años de trabajo meticuloso, sin una sola amonestación, sin un solo incidente de acceso indebido. Su reputación era, en muchos sentidos, su activo más valioso. Pero la reputación no servía de nada si el banco perdía dos mil millones de euros porque ella había preferido llenar un formulario antes que actuar.
Esperó a que el SOC se vaciara durante la pausa de almuerzo. Los analistas del turno de día salieron en grupo, como siempre, dejando atrás el zumbido de los

monitores y el brillo azul de los dashboards. Elena se quedó, diciendo que terminaría un informe. Nadie le preguntó nada.

Con la sala vacía, abrió la consola de administración de backups. El banco realizaba copias de seguridad automáticas de las configuraciones de sistema cada noche, incluyendo los repositorios de credenciales cifradas. Iván, como administrador, tenía sus claves de acceso almacenadas en un vault protegido por una contraseña maestra que solo él conocía. O eso se suponía.

Pero Elena sabía algo que Iván ignoraba: hacía seis meses, durante una auditoría de seguridad interna, ella había generado un diccionario de contraseñas personalizado para probar la robustez de los vaults de los administradores. El diccionario incluía combinaciones basadas en información personal de cada usuario: fechas, nombres de mascotas, lugares de nacimiento, datos que un atacante externo podría obtener mediante OSINT. Elena nunca había compartido los resultados de aquella auditoría con nadie, porque los resultados habían sido alarmantes: tres de cada cinco administradores usaban contraseñas de vault que su diccionario podía romper en menos de diez minutos.

Iván era uno de los tres.

Elena cargó el diccionario en la herramienta de descifrado y apuntó al backup del vault de Iván. El proceso comenzó: combinaciones probadas a una velocidad de miles por segundo, cada intento registrado en un log local que Elena borraría después. A los siete minutos y cuarenta y tres segundos, la herramienta se detuvo. La contraseña era el nombre de la hija de Iván seguido del año de nacimiento de su esposa.

El vault se abrió. Elena extrajo las credenciales de administrador con manos que le temblaban, no de miedo sino de la adrenalina fría de quien sabe que está cruzando una línea que no tiene retorno.

Con los privilegios de Iván, accedió al portátil de Marcos. No a la sesión activa —no quería que Marcos notara nada—, sino a la imagen forense del disco y al volcado de memoria RAM que el sistema realizaba automáticamente cada cuatro horas para diagnóstico de rendimiento. El último volcado era de las diez y veinte de la mañana, hacía tres horas.

Elena descargó el volcado a su estación de trabajo y lo cargó en un analizador de memoria. La herramienta recorrió los procesos activos, las conexiones de red, los manejadores de objetos, los hilos de ejecución. Elena filtró por procesos sin firma digital, conexiones a direcciones IP externas y módulos inyectados en procesos legítimos.

Lo encontró a los veinte minutos de análisis.

Un keylogger. No era un keylogger cualquiera: era una pieza de software modular, escrita en C y ensamblada con una precisión que Elena no había visto en muestras de malware común. Se había inyectado en el proceso del navegador web, capturando cada pulsación de teclado que Marcos hacía en sitios que coincidían con patrones de bancos, portales de autenticación y sistemas de transferencias. Los registros se cifraban en tiempo real y se exfiltraban mediante un canal encubierto embebido en consultas DNS, un técnica llamada DNS tunneling que era casi indetectable para los sistemas de monitorización de red.

El keylogger llevaba activo cuatro meses. Cuatro meses registrando cada pulsación de teclado del jefe de ciberseguridad del banco. Cuatro meses en los que Marcos había introducido, sin saberlo, sus credenciales

de acceso a sistemas críticos en un canal que alguien leía en tiempo real.
Elena se reclinó en la silla. La evidencia apuntaba en dos direcciones contradictorias: Marcos era víctima de un ataque sofisticado, o Marcos había instalado el keylogger él mismo para crear una coartada de compromiso. No podía determinar cuál de las dos era cierta con la información disponible.
Lo que sí podía determinar era que el atacante tenía ahora las credenciales de Marcos, y que con esas credenciales podía acceder a sistemas que Elena ni siquiera podía ver desde su consola.
Guardó el volcado de memoria en su unidad cifrada personal, borró los logs de su acceso al vault de Iván y cerró la consola de administración. El SOC seguía vacío. En la pantalla del SIEM, las microtransferencias a Singapur continuaban apareciendo a intervalos irregulares, como un pulso que no debía estar ahí.

Capítulo 4 — Código durmiente

Con las credenciales de Iván todavía activas en su sesión, Elena amplió el alcance de su análisis. Si el keylogger en el portátil de Marcos era solo una pieza de un rompecabezas mayor, lo más probable era que el atacante hubiera desplegado otros módulos en otros endpoints de la red corporativa. Los atacantes avanzados no se conformaban con un punto de entrada: se movían lateralmente, infectaban máquinas adicionales, establecían múltiples canales de comunicación para asegurar la persistencia incluso si una de las puertas traseras era descubierta y cerrada.
Configuró un escaneo silencioso de los endpoints corporativos. No un escaneo de puertos, que habría levantado alertas en el SIEM, sino una consulta pasiva a los registros de telemetría que cada equipo enviaba

al sistema central de monitorización: procesos activos, conexiones de red, consumo de CPU, firmas de archivos ejecutados. Elena buscaba patrones que indicaran la presencia de procesos que no deberían estar ahí, o procesos legítimos que se comportaban de manera anómala.

Los resultados llegaron en lotes. Doscientos cuarenta endpoints analizados. En doce de ellos, Elena encontró algo que no encajaba: un proceso llamado svchost-helper.exe que no estaba en la lista de binarios firmados por Microsoft y que se ejecutaba con privilegios de sistema. En condiciones normales, un proceso así habría sido detectado por el antivirus corporativo y puesto en cuarentena. Pero este proceso no estaba en la lista de amenazas conocidas, y su firma cambiaba cada doce horas.

Malware polimórfico. Cada doce horas, el código se reescribía a sí mismo: cambiaba la estructura de sus funciones, reordenaba sus instrucciones, alteraba las cadenas de texto que usaba como marcas internas. El resultado era un programa funcionalmente idéntico pero superficialmente distinto, una criptografía de la forma que engañaba a los sistemas de detección basados en firmas. El antivirus corporativo no lo reconocía porque cada versión era, para sus ojos, un programa nuevo.

Elena aisló una muestra del malware en un entorno sandbox: una máquina virtual aislada de la red corporativa, con herramientas de análisis forense y monitores de comportamiento. Ejecutó el binario y observó.

El malware se instaló como un servicio de Windows con un nombre que imitaba un servicio legítimo. Se conectó a un servidor de command and control mediante una conexión HTTPS encriptada que, desde fuera, parecía tráfico web normal. Luego, se quedó

quieto. No hizo nada. No ejecutó comandos, no exfiltró datos, no se propagó a otras máquinas. Simplemente esperó.
Código durmiente. Un sleeper agent que permanecía inactivo hasta recibir una señal de activación.
Elena examinó el código del módulo de comunicación. Encontró la lógica de activación: el malware esperaba una señal específica, un paquete de datos con una estructura particular que llegaría a través de una consulta DNS a un dominio concreto. Cuando la señal llegara, el malware ejecutaría su módulo de exfiltración: recopilaría archivos de un conjunto de rutas predefinidas, los comprimiría, los cifraría y los enviaría al servidor de command and control en fragmentos camuflados como tráfico DNS.
Las rutas predefinidas eran directorios del sistema de transferencias SWIFT.
Elena sintió un frío que no tenía nada que ver con el aire acondicionado del SOC. El atacante había preparado un mecanismo de exfiltración programado para vaciar el sistema de transferencias. Solo faltaba la señal de activación.
Examinó el timestamp del último cambio de firma del malware. La mutación había ocurrido a las seis de la mañana. La siguiente estaba programada para las seis de la tarde. Y en el código, Elena encontró un contador de iteraciones: el malware estaba programado para ejecutar su módulo de exfiltración después de la iteración número catorce. La iteración actual era la trece.
La señal de activación llegaría en la siguiente mutación: el viernes a medianoche.
Elena estaba anotando estos datos cuando la puerta del SOC se abrió. No fueron los analistas del turno de día, que aún no habían vuelto del almuerzo. Era Lucía Ferrer, responsable de compliance del banco, con una

carpeta bajo el brazo y una expresión que Elena reconoció de inmediato: la expresión de alguien que ha encontrado una discrepancia en un log de acceso y ha venido a pedir explicaciones.

—Elena Vega —dijo Lucía, con la voz mesurada que usaba en las auditorías—. ¿Puedes explicarme por qué tu cuenta ha accedido a la consola de administración de backups a las trece y cuarenta y siete de esta tarde?

No era una pregunta. Era una apertura de expediente. Elena valoró sus opciones durante dos segundos. Mentir era inútil: Lucía tenía los logs. Negar era contraproducente: solo retrasaría lo inevitable. La única opción viable era la verdad parcial.

—Estoy investigando una posible intrusión —dijo Elena —. Necesitaba acceso a una imagen forense y no podía esperar a los canales regulares.

—¿Con autorización de quién?

—De nadie.

Lucía asintió lentamente, como si la respuesta no la sorprendiera.

—Lo que has hecho es una violación del protocolo de acceso. Podría escalar esto a Dirección ahora mismo, y 你知道吗 estarías fuera del edificio antes de que terminara el día.

—Puedes hacerlo. Pero antes deberías ver esto.

Elena giró su monitor hacia Lucía. En la pantalla: el análisis del malware polimórfico, las doce máquinas infectadas, el módulo de exfiltración programado para el viernes. Lucía observó en silencio durante un minuto. Su expresión pasó de la severidad burocrática a algo que Elena no le había visto antes: preocupación genuina.

—¿Esto es real?

—Es real.

—¿Marcos lo sabe?
—Le informé de la anomalía inicial anoche. La descartó.
Lucía se quedó callada un momento. Luego dijo:
—Te doy cuarenta y ocho horas. Si para el jueves al mediodía no tienes un informe completo que justifique esto, lo escalo a Dirección y asumo las consecuencias. Pero si esto que dices es cierto, el banco entero está en peligro.
Elena asintió. Lucía se dio la vuelta y salió del SOC con el mismo paso medido con el que había entrado, pero Elena notó que apretaba la carpeta con más fuerza de la necesaria.
Cuando se quedó sola, Elena volvió a la sandbox. El malware seguía durmiendo, esperando su señal. El viernes a medianoche. Faltaban setenta y dos horas.

Capítulo 5 — Llaves falsas

El problema de las credenciales robadas era que eran, desde el punto de vista del sistema, credenciales legítimas. El sistema IAM del banco —Identity and Access Management— no detectaba anomalías en los accesos del atacante porque estos usaban cuentas reales, con permisos reales, desde direcciones IP que pertenecían a la red corporativa. Para el IAM, no había diferencia entre Marcos Durán iniciando sesión desde su oficina y un atacante usando las credenciales robadas de Marcos Durán desde una máquina comprometida en la misma red.
La autenticación, por sí sola, no era suficiente. Elena necesitaba contexto: no solo quién se conectaba, sino desde dónde, cuándo, y cómo.
Cruzó los logs de login del sistema con los registros de acceso físico al edificio. El banco usaba tarjetas de proximidad para controlar el acceso a las distintas

zonas de la sede, y cada vez que alguien pasaba una tarjeta por un lector, el evento se registraba en la base de datos de control físico. En teoría, si un empleado iniciaba sesión en un sistema desde la oficina de Madrid, su tarjeta debería haber registrado una entrada en el edificio de Madrid esa misma mañana.

Las discrepancias comenzaron a aparecer en el tercer cruce.

Una cuenta de administrador de sistemas se había conectado al servidor de transferencias desde la red de la oficina de Madrid a las nueve y veinte de la mañana del martes. Pero la tarjeta asociada a ese empleado había registrado una entrada en la oficina de Lisboa a las ocho y cinco de esa misma mañana. Era físicamente imposible que la persona hubiera estado en ambos lugares.

La cuenta pertenecía a Daniel Reyes, arquitecto de sistemas del banco. Elena revisó su perfil: treinta y cuatro años, siete años en la entidad, acceso a infraestructura crítica, participó en el diseño de la arquitectura de red del data center. Un perfil que, si era cómplice, representaba una amenaza de primer nivel.

Pero Elena también encontró que Daniel había viajado a Lisboa para una conferencia de seguridad el lunes, y que su billete de vuelta era para el miércoles. El martes, cuando su cuenta se conectó desde Madrid, Daniel estaba físicamente en Lisboa, en la conferencia, con su tarjeta de acceso registrando entradas y salidas en el edificio portugués.

Las credenciales de Daniel habían sido clonadas. Pero, ¿cómo?

Elena profundizó en el análisis. Los registros de autenticación mostraban que la cuenta de Daniel se había autenticado en Madrid usando un hash de contraseña válido. No había habido un intento de login fallido, ni un cambio de contraseña, ni una alerta de

seguridad. El sistema había aceptado el hash como legítimo porque lo era. Pero el hash no había sido introducido por Daniel: había sido extraído de la memoria de un equipo comprometido y reutilizado mediante una técnica llamada pass-the-hash.

El ataque había ocurrido semanas antes. Elena rastreó el origen hasta uno de los doce endpoints infectados con el malware polimórfico. Esa máquina, a su vez, había sido comprometida mediante el keylogger que Elena había encontrado en el portátil de Marcos. La cadena de compromiso era clara: el atacante había usado el keylogger para capturar credenciales, había usado esas credenciales para moverse lateralmente, había infectado máquinas adicionales, y desde una de esas máquinas había extraído el hash de Daniel mediante un ataque de robo de credenciales en memoria.

Daniel no era el infiltrado. Daniel era una víctima cuyas llaves habían sido copiadas sin que él lo supiera.

Elena necesitaba confirmarlo. Lo encontró en la cafetería del banco, sentado solo con un café y un portátil, revisando las presentaciones de la conferencia de Lisboa.

—¿Mind if I sit? —preguntó Elena, usando el inglés que Daniel prefería para conversaciones informales.

—Sure.

Se sentó frente a él con un café que no pensaba beber. Conversaron durante diez minutos sobre la conferencia, sobre las tendencias en arquitectura de seguridad, sobre un proveedor que había presentado una solución de zero trust que Elena consideraba sobrevalorada. Luego, con la naturalidad de quien cambia de tema sin razón aparente, Elena preguntó:

—¿Alguna vez has dejado tu portátil en la oficina sin cerrar sesión?

Daniel la miró con sorpresa.

—Siempre lo bloqueo. Política de seguridad, ¿no?
—¿Y en Lisboa? ¿El portátil viajó contigo?
—No, lo dejé en la oficina. Solo me llevé el móvil. ¿Por qué?
Elena no podía revelarle lo que había descubierto. No todavía. Pero la respuesta de Daniel confirmaba lo que ella ya sospechaba: el portátil de Daniel se había quedado en Madrid, en la oficina, y alguien con acceso físico lo había usado para extraer el hash de sus credenciales mientras Daniel estaba en otra país.
—Solo una rutina de auditoría —dijo Elena—. Nada importante.
Daniel la miró con desconfianza, pero no insistió. Elena se despidió y salió de la cafetería con una certeza que la helaba: el atacante no era Daniel, pero tenía las llaves de Daniel, y esas llaves abrían puertas a las que Elena ni siquiera podía asomarse.
El verdadero infiltrado seguía oculto. Y tenía acceso a cuentas privilegiadas.

Capítulo 6 — La llave maestra

Para ejecutar la transferencia masiva, el atacante necesitaba algo más que credenciales de administrador. Necesitaba las claves de cifrado del sistema de transferencias SWIFT del banco. Esas claves eran la última barrera: sin ellas, era imposible autorizar una transferencia internacional desde la entidad. Y esas claves no estaban en un solo lugar.
El banco usaba un esquema de Shamir para proteger las claves SWIFT. El esquema, basado en la criptografía de secreto compartido, dividía la clave maestra en tres fragmentos matemáticamente vinculados. Cada fragmento era custodiado por una persona diferente. Para reconstruir la clave completa y autorizar una transferencia, se necesitaban al menos

dos de los tres fragmentos. Un solo custodio no podía hacerlo. Dos sí.

Elena había revisado el protocolo de custodia: los tres custodios eran Marcos Durán, el CEO Alejandro Vidal, y Carmen Ibarra, ejecutiva de riesgo operativo. Tres personas, tres fragmentos, dos necesarios para abrir la caja fuerte digital.

Si el atacante quería ejecutar la transferencia, necesitaba comprometer al menos a dos de los tres custodios. Marcos ya estaba comprometido: su keylogger había estado capturando pulsaciones durante meses, y Elena no podía descartar la posibilidad de que el fragmento de Marcos estuviera ya en manos del atacante. ¿Pero quién era el segundo?

Elena pensó en Carmen Ibarra. Ejecutiva de riesgo, cincuenta y dos años, veintitrés años en el banco, reputación intachable. Pensó en Alejandro Vidal, el CEO, un hombre que delegaba la mayoría de las decisiones técnicas y que rara vez interactuaba con los sistemas directamente. Vidal era un objetivo difícil: no usaba sistemas críticos en su día a día, y sus hábitos digitales eran mínimos. Carmen, en cambio, era una usuaria activa de los sistemas internos, participaba en revisiones de seguridad, accedía a plataformas de gestión de riesgos.

Elena necesitaba saber cuál de los dos estaba siendo atacado. Y para eso, necesitaba monitorizar sus estaciones de trabajo.

Instalar un monitor de actividad en los puestos de los tres custodios era, técnicamente, una operación de espionaje interno. No estaba autorizada por ningún protocolo. No tenía justificación formal. Si la descubrían, no sería un expediente disciplinario: sería un despido inmediato y probablemente una demanda. Lo hizo de todos modos.

Usó las credenciales de Iván para acceder remotamente a los tres equipos durante la madrugada del miércoles. En cada uno, instaló un agente de monitorización silencioso que registraba procesos activos, conexiones de red, pulsaciones de teclado y accesos a archivos. El agente enviaba los datos a un servidor local que Elena había configurado en una máquina virtual aislada, fuera del alcance del SIEM.
Mientras instalaba el agente en el equipo de Carmen, Elena notó algo en el historial de navegación: Carmen había visitado, la semana anterior, un portal de soporte técnico que no correspondía a ningún proveedor conocido del banco. El dominio estaba registrado hacía quince días, con un certificado SSL de validación básica y una página que imitaba la estética de un portal corporativo. Era una página de phishing, pero no dirigida a capturar credenciales: estaba diseñada para descargar un payload silencioso aprovechando una vulnerabilidad del navegador.
Carmen había sido atacada. Pero, ¿había caído?
Elena no podía saberlo todavía. El agente de monitorización necesitaba tiempo para recopilar datos. Mientras esperaba, su mente se deslizó por un camino que prefería no transitar.
Marcos.
No solo su jefe. No solo su colega de profesión. Hacía seis años, antes de que Elena se incorporara al banco, habían tenido una relación. Había durado ocho meses: cenas tardías después de jornadas maratonianas, conversaciones sobre amenazas y arquitecturas de seguridad que se convertían en confesiones personales, una intimidad construida sobre la base compartida de dos personas que vivían en el mismo mundo de alertas y vulnerabilidades. La relación había terminado mal: Marcos era incapaz de separar el trabajo de la vida personal, y Elena había descubierto

que la confianza que le otorgaba en la cama no se extendía al despacho, donde Marcos la trataba con la misma condescendencia profesional que al resto del equipo.
Elena se había prometido a sí misma que aquel pasado no afectaría su juicio. Pero la duda era como un parásito: se alimentaba de la incertidumbre. ¿Y si Marcos no era víctima? ¿Y si el keylogger en su portátil era una coartada? ¿Y si su actitud minimizadora ante las alertas no era negligencia, sino complicidad?
Se obligó a volver al presente. A los datos. A lo que podía verificar.
A las tres de la madrugada del jueves, el agente de monitorización registró un evento en el equipo de Carmen Ibarra. Alguien había accedido al módulo de gestión de claves SWIFT desde una sesión remota iniciada a las 02:47. La sesión usaba credenciales válidas de Carmen, pero se originaba desde una dirección IP que no pertenecía a la red corporativa del banco. Era una conexión VPN desde un servidor externo, enrutada a través de un proveedor de servicios en un país que Elena no reconoció de inmediato.
Carmen no estaba en la oficina a las tres de la madrugada. Pero alguien estaba usando sus credenciales para acceder al módulo de claves.
El segundo custodio había sido comprometido.

Capítulo 7 — Contención

Elena ya no podía operar en solitario. La escala de la amenaza, la sofisticación del ataque y la inminencia del plazo la obligaban a romper el silencio y activar el protocolo formal de respuesta a incidentes.
Fue a ver a Lucía Ferrer antes de que el turno de mañana comenzara. La encontró en su despacho,

revisando correos con una taza de té que despedía vapor en la luz fría de las pantallas. Lucía la miró con una mezcla de recelo y preocupación: la misma mezcla que había mostrado cuarenta y ocho horas antes, cuando Elena le había revelado la existencia del malware polimórmico.

—Necesito que activemos el protocolo de respuesta a incidentes —dijo Elena sin preámbulo—. Nivel crítico.

—Siéntate.

—No puedo sentarme. Tenemos menos de cuarenta y ocho horas antes de que el atacante ejecute una transferencia de dos mil millones de euros.

Lucía dejó la taza. Su rostro adoptó la expresión de eficiencia burocrática que Elena había aprendido a respetar: no era empatía ni miedo, era la concentración de alguien que ha aprendido a operar bajo presión institucional.

—Explícame todo. Desde el principio.

Elena le contó todo. Las microtransferencias, el keylogger, el malware polimórfico, las credenciales clonadas de Daniel Reyes, el acceso no autorizado al módulo de claves SWIFT desde el equipo de Carmen. Omitió solo dos cosas: que había usado las credenciales robadas de Iván, y que conservaba copias de la evidencia en su unidad cifrada personal. Algunas confesiones podían esperar.

Lucía escuchó sin interrumpir. Cuando Elena terminó, permaneció en silencio durante treinta segundos.

—¿Quién más sabe esto?

—Nadie. Solo tú.

—Necesitamos un equipo de crisis. Reducido. Confiable.

En dos horas, Lucía había convocado a Tomás Bravo, un CISO externo que trabajaba como consultor de seguridad para varios bancos europeos y que tenía un historial de gestión de incidentes críticos. Con él llegó

un abogado corporativo del bufete que asesoraba al banco, un hombre discreto llamado Adrián Vega —sin relación alguna con Elena— que se especializaba en derecho tecnológico y gestión de crisis.

El equipo se reunió en una sala de conferencias del piso ejecutivo, a puerta cerrada, sin teléfonos móviles. Elena presentó la evidencia. Tomás Bravo la interrumpió varias veces para pedir aclaraciones técnicas; el abogado tomó notas sin levantar la vista. Cuando terminó, Lucía propuso lo que Elena ya sabía que era necesario: interrogar a Carmen Ibarra.

La trajeron a la sala quince minutos después. Carmen entró con el rostro pálido y los ojos enrojecidos de quien no ha dormido. Se sentó al extremo de la mesa, con las manos entrelazadas sobre el tablero, y miró a Elena con una expresión que no era de culpa sino de agotamiento.

—Sé por qué estoy aquí —dijo antes de que nadie abriera la boca—. Sé qué encontrasteis.

Lucía tomó la palabra.

—Carmen, necesitamos que nos expliques qué ha ocurrido.

Carmen habló durante veinte minutos. Su voz era monocorde, como si estuviera recitando un relato que había ensayado en su cabeza durante días.

Hacía tres semanas, había recibido una videollamada en su número personal. La persona al otro lado era su hija. O lo parecía: misma cara, misma voz, mismo gesto de tocarse el pelo detrás de la oreja cuando estaba nerviosa. La hija de Carmen estaba en el extranjero, estudiando un máster. En la videollamada, le dijo que estaba en peligro, que unas personas la habían secuestrado, que necesitaba que su madre hiciera algo para protegerla. Le dio instrucciones: acceder a un portal, descargar un archivo, ejecutarlo en su equipo de trabajo. La videollamada duró cuatro minutos.

Carmen hizo lo que le pidieron. Cuando accedió al portal, descargó el archivo y lo ejecutó, no pasó nada visible. Su equipo siguió funcionando con normalidad. Durante los días siguientes, recibió más instrucciones: acceder al módulo de gestión de claves en horarios específicos, introducir su fragmento de clave en un proceso de validación que le fue presentado como una rutina de seguridad. Cumplió cada instrucción.

Luego, hace una semana, su hija la llamó. Estaba bien. Nunca había sido secuestrada. La videollamada era un deepfake: una síntesis de vídeo y audio generada por inteligencia artificial que había replicado su rostro, su voz y sus gestos con una precisión que Carmen, incluso sabiendo la verdad, no podía distinguir del original.

El secuestro había sido virtual. La manipulación, absoluta.

Silencio en la sala. Tomás Bravo fue el primero en hablar.

—Esto no es un ataque ordinario —dijo—. La sofisticación del deepfake, la cadencia de las instrucciones, el uso de técnicas psicológicas de coerción... Esto es un APT. Advanced Persistent Threat. Hablamos de un grupo con recursos de nivel estatal o de crimen organizado de alta gama. No son script kiddies. No son cibercriminales comunes. Son profesionales.

—¿Qué opciones tenemos? —preguntó Lucía.

—Dos —respondió Tomás—. Opción A: cerramos los sistemas de transferencias ahora mismo. Desconectamos el banco de la red SWIFT, bloqueamos todas las transferencias pendientes, activamos el protocolo de emergencia. El atacante no podrá ejecutar la transferencia. Pero el banco dejará de operar durante al menos cuarenta y ocho horas, las pérdidas por operaciones interrumpidas serán millonarias, y cuando

la noticia se filtre —porque se filtrará— el pánico será peor que el daño directo.
—¿Opción B?
—Dejamos que el ataque avance. Tendemos una trampa. Redirigimos la transferencia a una cuenta controlada por las autoridades y capturamos al infiltrado interno cuando intente ejecutar la fase final.
—Eso requiere que el atacante crea que todo está funcionando —dijo Elena—. Y requiere que identifiquemos al infiltrado antes del viernes a medianoche. Si nos equivocamos, perdemos dos mil millones.
Tomás la miró.
—¿Tienes una alternativa mejor?
Elena no la tenía.
—La trampa —dijo Lucía—. Pero necesitamos al infiltrado.

Capítulo 8 — Caza al cazador

Para tender la trampa, Elena necesitaba pensar como el atacante. No como un defensor que reacciona a amenazas, sino como un atacante que planifica movimientos. Era un ejercicio de red team: ponerse en el lugar del adversario, recorrer su camino, anticipar su siguiente paso.
Se encerró en una sala de reuniones vacía con una pizarra blanca y un portátil. Dibujó la topología de la red del banco: los segmentos, los firewalls, los servidores, el data center. Trazó con un rotulador rojo el camino que el atacante había seguido hasta ahora: entrada por phishing, keylogger en el equipo de Marcos, robo de credenciales, movimiento lateral, malware polimórfico, compromiso de Carmen, acceso al módulo de claves.

El atacante tenía los fragmentos de clave de Marcos y Carmen. Tenía credenciales de administrador. Tenía un malware de exfiltración programado para el viernes a medianoche. ¿Qué le faltaba?

Elena estudió el diseño del sistema de transferencias SWIFT del banco. Para ejecutar una transferencia autorizada, el sistema requería tres factores: las claves de cifrado reconstruidas, una autorización digital firmada por un custodio con biometría, y un acceso físico al servidor de transacciones en el data center.

Las claves podían reconstruirse con los fragmentos de Marcos y Carmen. La biometría podía obtenerse de Marcos, si era cómplice, o forzarse mediante un ataque de suplantación si el atacante tenía acceso a los datos biométricos de algún custodio.

Pero el acceso físico era la pieza crítica. El servidor de transacciones estaba en una sala cerrada dentro del data center, protegida por una puerta biométrica que requería la huella dactilar de un operador autorizado. El atacante necesitaba a alguien dentro del edificio, con acceso físico, que pudiera llegar a esa sala.

Elena revisó la lista de personas con acceso biométrico a la sala de servidores de transacciones. Eran cinco: Marcos, Iván Soler, Daniel Reyes, un operador de data center llamado Raúl Mengíbar, y un técnico de mantenimiento externo de la empresa proveedora del hardware, contratado bajo acuerdo de servicios.

El técnico externo. Elena había pasado por alto ese perfil porque no era un empleado del banco. Pero tenía acceso físico, tenía huella registrada en el sistema biométrico, y tenía una razón legítima para entrar en el data center.

Instalaron cámaras adicionales en el pasillo de acceso al data center y en la antecámara de la sala de servidores. Elena configuró un monitor de eventos que alertaría en tiempo real si la puerta biométrica se

activaba fuera de los horarios programados de mantenimiento. El equipo de crisis se turnó para vigilar las cámaras en turnos de cuatro horas.
Mientras esperaban, Tomás Bravo abordó a Elena en el pasillo.
—Necesito preguntarte algo —dijo—. ¿Desde cuándo estás operando fuera de protocolo?
—¿Perdón?
—Lucía me ha puesto al día. Accediste al vault de Iván. Instalaste monitores en los equipos de los custodios sin autorización. Guardaste evidencia en un dispositivo personal. Cada una de esas acciones es una violación de política interna. Si esto llega a un tribunal, tu cadena de custodia es indefendible.
Elena lo miró con calma.
—Lo sé.
—¿Y lo hiciste de todos modos.
—Si hubiera seguido el protocolo, estaríamos esperando la aprobación de un comité mientras el atacante vacía el banco. No tenía tiempo para ser correcta. Tenía tiempo para ser eficaz.
Tomás la estudió durante un momento.
—Eso no será suficiente para un juez.
—No estoy pensando en jueces. Estoy pensando en el viernes a medianoche.
Tomás no respondió. Elena volvió a la sala de monitorización.
El jueves, a las once y cuarenta de la noche, la alarma se activó. Alguien había presentado una credencia biométrica válida en la puerta de la sala de servidores de transacciones. La huella coincidía con el perfil de Iván Soler.
Pero Iván Soler seguía en Tenerife.
Elena y Lucía se precipitaron al data center por separado: Elena por el pasillo principal, Lucía por la escalera de emergencia. Cuando Elena llegó a la

antecámara, encontró a un hombre vestido con el uniforme de la empresa proveedora de servicios técnicos, de rodillas frente a la puerta biométrica, intentando conectar un dispositivo al lector de huellas.
—No te muevas —dijo Elena.
El hombre levantó las manos. No era Iván. Era el técnico de mantenimiento externo, un hombre de unos cuarenta años con el rostro desencajado por el miedo.
Lucía apareció por la escalera treinta segundos después.
Lo llevaron a una sala de reuniones. El hombre habló con la rapidez de quien espera que las palabras sirvan de escudo.
—No soy yo. Quiero decir, soy yo, pero no es idea mía. Recibo instrucciones. Pagos a una cuenta. Cada vez que hay un trabajo, recibo un mensaje con instrucciones y una fecha. No conozco a la persona que me envía los mensajes. Solo conozco un alias.
—¿Qué alias? —preguntó Elena.
—Arquitecto. Me dicen que es el Arquitecto quien da las órdenes.
Elena sintió que las piezas encajaban, pero la imagen que formaban no era la que esperaba.
Arquitecto. Un alias interno. Alguien con conocimiento profundo de la arquitectura de sistemas del banco. Alguien que conocía los protocolos, las debilidades, los nombres de los custodios, los horarios de mantenimiento, las rutas de acceso.
Alguien que llevaba meses, quizá años, planificando esto.

Capítulo 9 — El arquitecto

Arquitecto. Elena recorrió mentalmente la lista de perfiles del banco que incluían ese título o uno equivalente. Arquitecto de sistemas: Daniel Reyes,

descartado. Arquitecto de datos: una mujer llamada Sara Kowalski, que llevaba tres meses de baja médica y no tenía acceso a sistemas críticos. Arquitecto de seguridad: un puesto que había sido eliminado en la última reorganización. Arquitecto de infraestructura... Elena se detuvo.

Arquitecto de infraestructura. Era el puesto que Marcos Durán había ocupado antes de ser ascendido a jefe de ciberseguridad, hacía cuatro años. En aquel rol, Marcos había diseñado la topología de red del data center, había definido los protocolos de acceso biométrico, había seleccionado los sistemas de monitorización y había configurado los segmentos de red que ahora protegían —en teoría— los sistemas críticos del banco. Marcos conocía el edificio como nadie. Conocía cada cable, cada servidor, cada punto de acceso. Conocía las debilidades de los protocolos porque él mismo los había escrito. Y conocía las debilidades del SIEM porque había sido él quien lo había configurado.

Elena pensó en el keylogger en su portátil. Cuatro meses activo. ¿Era posible que Marcos no se hubiera dado cuenta? ¿O era posible que lo hubiera instalado él mismo, como coartada, para poder argumentar que había sido víctima de un ataque?

Pensó en su respuesta a la alerta inicial: "Llevas demasiadas noches sin dormir". ¿Era preocupación genuina, o un intento de apartarla de la investigación?

Pensó en los detalles del malware polimórfico que Marcos conocía. Detalles que Elena no había compartido en ningún informe oficial. Detalles que solo alguien con acceso a la muestra aislada podría conocer. Y, sin embargo, Marcos los había mencionado en una conversación casual esa misma mañana, como si los conociera de antes.

Elena fue a su oficina. No con un plan, sino con una necesidad que no podía posponer: mirarlo a la cara y preguntar.

Marcos estaba en su despacho, frente a un portátil, con una taza de café y una pila de informes sobre la mesa. La recibió con una sonrisa que Elena ya no sabía si leer como cordialidad o máscara.

—Necesito hablar contigo —dijo Elena—.Sobre el ataque.

—¿Qué ataque?

—El que estás coordinando. Arquitecto.

La sonrisa de Marcos se congeló. No desapareció: se solidificó, como una expresión tallada en piedra. Elena cerró la puerta detrás de ella.

—No sé de qué hablas —dijo Marcos.

—Sé que fuiste arquitecto de infraestructura antes de este puesto. Sé que el alias que usa el técnico de mantenimiento es «Arquitecto». Sé que conoces detalles del malware polimórfico que no se han compartido en ningún informe. Y sé que el keylogger en tu portátil puede ser una coartada, no una evidencia de ataque.

Marcos la miró durante un largo momento. Luego, algo cambió en su rostro. No fue una confesión dramática: fue un desmoronamiento lento, como un muro que cede por dentro mientras mantiene su fachada.

—¿Cómo lo supiste?

—No lo sabía con certeza. Hasta ahora.

Marcos se dejó caer en la silla. Pasó las manos por el rostro. Cuando habló, su voz había perdido toda la autoridad que Elena le había conocido.

—Fue hace dos años. Tenía deudas. Juego. Cantidades que no podía pagar. Me abordaron en una cena, en un evento del sector. No sé cómo supieron de las deudas. Alguien que conocía a alguien. Me ofrecieron una salida: filtrar información menor, nada

crítico, nada que pudiera dañar al banco. Solo datos de configuración, mapas de red, listas de empleados. A cambio, mis deudas desaparecían.
—Y aceptaste.
—Acepté. Y luego me pidieron más. Siempre más. Cada paso era más grande, más comprometedor. No podía salirme porque tenían evidencia de todo lo anterior. Estaba atrapado.
Elena lo escuchó sin piedad. No porque no sintiera compasión, sino porque la compasión habría sido un lujo que no podía permitirse.
—El ataque del viernes —dijo—. ¿Cuál es tu rol?
—Mi biometría. El sistema de transferencias requiere la autorización biométrica de un custodio para validar la transacción final. Yo soy ese custodio. El ataque no puede ejecutarse sin mi huella.
—¿Y estás dispuesto a hacerlo?
—No tengo elección. Si no cumplo, publican la evidencia. Pierdo todo. Familia, carrera, libertad.
Elena sacó su móvil del bolsillo. Debajo de la mesa, donde Marcos no podía verlo, había activado la grabación de audio antes de entrar.
—Puedo protegerte —dijo Marcos, con la urgencia de quien ve el abismo acercarse—. Si me garantizas que hablaré con la fiscalía, que puedo cooperar, que... puedo entregar a la gente que está detrás de esto. Pero necesito protección. Necesito que no me procesen.
—No puedo prometerte eso.
—Entonces estamos perdidos los dos.
Elena se levantó.
—La transferencia está programada para las once cincuenta y nueve del viernes. Tu biometría es la última pieza. Si cooperas, si dejas que la operación continúe bajo nuestro control, podemos redirigir los fondos y capturar a las personas que te reclutaron. Si no

cooperas, cerraré los sistemas yo misma y dejaré que la evidencia hable por sí sola.
Marcos la miró desde la silla, con los ojos de alguien que ha comprendido que todas las salidas conducen al mismo lugar.
—Cooperaré —dijo.
Elena salió del despacho con la grabación en su móvil y la última pieza del rompecabezas en su poder. Faltaban veinticuatro horas para el viernes a medianoche.

Capítulo 10 — Resiliencia

Viernes. Veintidós horas.
El data center subterráneo del Banco Europeo Meridional tenía la temperatura de una nevera industrial y el silencio de una catedral vacía. Solo el zumbido de los servidores, constante y casi litúrgico, rompía la quietud. Elena llevaba dieciséis horas seguidas en el SOC, alternando entre la sala de monitorización y la sala de crisis que se había convertido en su cuartel general.
El plan era sencillo en concepto y demoníaco en ejecución. Dejarían que Marcos autorizara la transferencia con su biometría. El sistema aceptaría la transacción, pero el equipo de Elena habría redirigido previamente las cuentas de destino a una cuenta controlada por las autoridades, registrada a nombre de una entidad judicial que cooperaba con la operación. Cuando el atacante remoto recibiera la confirmación de transferencia y viera que los fondos no llegaban a sus cuentas, intentaría abortar. En ese momento, el equipo capturaría los logs de comunicación, las direcciones IP del servidor de command and control, y cualquier huella que el atacante dejara en su intento de retirada.

Elena había rehecho la configuración del módulo de exfiltración del malware polimórfico. En lugar de enviar datos al servidor de command and control original, redirigiría el tráfico a un honeypot de red donde cada paquete sería capturado y analizado. Tomás Bravo había coordinado con las autoridades judiciales para asegurar que la cuenta receptora estuviera lista. Lucía había preparado la documentación legal para la operación.

Marcos estaba en una sala contigua, con un agente de seguridad en la puerta. Había aceptado la operación con la resignación de un hombre que ha agotado sus opciones.

A las veintitrés horas, Elena hizo una verificación final de todos los sistemas. La redirección de cuentas: activa. El honeypot de exfiltración: activo. La monitorización de la conexión del atacante: activa. Las cámaras del data center: grabando.

A las veintitrés treinta, Marcos fue escoltado al lector biométrico de la sala de servidores de transacciones. Elena lo observó por la cámara: se veía pequeño, menguado, con las manos temblorosas. Presentó su huella. El sistema la validó.

A las veintitrés cuarenta, el módulo de transferencias SWIFT se activó. Elena vio en su consola cómo el sistema iniciaba el proceso de autorización: validación de claves, reconstrucción del secreto compartido de Shamir con los fragmentos de Marcos y Carmen, verificación biométrica. Cada paso se ejecutó sin errores. El sistema creía que todo era legítimo.

A las veintitrés cuarenta y cinco, la primera señal de problema apareció.

El servidor de command and control del atacante envió una consulta de estado. El honeypot respondió con los datos esperados. Pero la consulta incluía un campo de verificación que Elena no había previsto: un checksum

que validaba la integridad de la ruta de exfiltración. El checksum no coincidía, porque la ruta había sido redirigida.
El atacante lo supo en segundos.
A las veintitrés cuarenta y siete, el sistema de transferencias registró un intento de cancelación. El atacante intentaba abortar la transacción antes de que se completara. Elena bloqueó la cancelación: la transferencia ya estaba en proceso de validación final y no podía interrumpirse sin autorización de dos custodios.
A las veintitrés cuarenta y nueve, el atacante cambió de estrategia. Dejó de intentar cancelar la transferencia y se centró en destruir la evidencia. Elena vio en su consola cómo se ejecutaban comandos de limpieza en los endpoints infectados: los doce equipos con malware polimórfico comenzaron a sobrescribir sus sectores de disco, borrando rastros del código malicioso.
El atacante estaba quemando el campo. Destruía todo lo que podía mientras intentaba mantener una conexión de salida.
Elena actuó por instinto. Aisló los endpoints de la red, cortando su conexión externa antes de que la limpieza se completara. En tres de los doce equipos, los comandos de borrado no llegaron a ejecutarse por completo. La evidencia del malware, de las conexiones al servidor de command and control y de los módulos de exfiltración se preservó.
A las veintitrés cincuenta y tres, el atacante intentó acceder directamente al sistema de logs central para borrar el registro de la transferencia. Elena ya había anticipado este movimiento: había configurado una réplica de los logs en un servidor aislado, fuera del alcance de cualquier cuenta comprometida. El atacante pudo borrar los logs primarios, pero no la réplica.

A las veintitrés cincuenta y siete, el sistema de transferencias SWIFT completó la validación final. La transferencia de dos mil millones de euros fue autorizada y ejecutada. Los fondos no fueron a las cuentas de Singapur del atacante: fueron a la cuenta judicial controlada por las autoridades.

A las veintitrés cincuenta y nueve, el atacante cortó todas las conexiones. Los servidores de command and control dejaron de responder. Las cuentas de correo usadas para las instrucciones al técnico de mantenimiento fueron canceladas. El rastro digital que el atacante había dejado durante meses se desvaneció en menos de un minuto.

Elena se quedó en su consola, respirando con dificultad, con las manos temblorosas sobre el teclado. La pantalla mostraba la confirmación de transferencia, los logs preservados y la lista de endpoints aislados. La transferencia había sido interceptada. Los fondos estaban a salvo. Marcos había sido detenido en la sala de servidores por los agentes que lo escoltaban.

Pero el atacante remoto, la mente detrás de la operación, había desaparecido.

El amanecer del sábado entró por las ventanas del SOC como una intrusión. Una luz cálida y ajena que no combinaba con el frío azul de las pantallas. Elena llevaba treinta horas despierta, y el cansancio había dejado de ser una sensación para convertirse en un estado del ser: una niebla que ocupaba el espacio entre sus pensamientos y el mundo.

Lucía entró en el SOC con dos cafés. Le ofreció uno sin decir nada. Elena lo aceptó sin decir nada. Bebieron en silencio, de pie frente a la ventana, mirando la ciudad que despertaba ajena a lo que había ocurrido en las últimas setenta y dos horas.

—El banco sobrevivió —dijo Lucía.

—Sí.

—Pero la confianza no.
Elena no respondió. Sabía que Lucía tenía razón. Se podía recuperar el dinero, preservar la evidencia, detener al cómplice interno. Pero la idea de que el jefe de ciberseguridad hubiera sido el autor del ataque, de que el sistema había estado protegido por alguien que lo estaba vulnerando, era una grieta que ningún parche técnico podía sellar.
Lucía se fue. Elena se quedó en la ventana. Su móvil vibró en el bolsillo. Era un mensaje de Tomás Bravo, ofreciéndole la dirección de un nuevo equipo de respuesta a amenazas internas que el banco quería crear. Un ascenso, en teoría. El reconocimiento de que ella había salvado la entidad.
Elena leyó el mensaje sin responder. No sabía si aceptar. No sabía si quería seguir en un mundo donde la mayor amenaza no venía de fuera, sino de la silla de al lado.
Pensó en el mensaje anónimo del lunes: *Deja de mirar donde no debes.* Nunca se había rastreado el número. La investigación sobre el técnico de mantenimiento había revelado una cadena de intermediarios que se perdía en jurisdicciones donde las peticiones de cooperación judicial tardaban años. Marcos había confesado su rol, pero no conocía a las personas que lo habían reclutado más allá de alias y comunicaciones cifradas.
El verdadero Arquitecto seguía libre. El plan de robo había fracasado, pero el conocimiento que el atacante había acumulado sobre el banco, sobre sus sistemas, sobre sus personas, seguía existiendo en algún servidor, en alguna mente, en alguna sombra.
Elena guardó el móvil. Recogió su unidad cifrada personal del cajón de su escritorio y la sostuvo en la mano, sintiendo su peso insignificante. Dentro de ella estaban todas las pruebas que había reunido, todos los

datos que había extraído saltándose protocolos. Si la entregaba, la evidencia sería formalmente admisible pero ella enfrentaría consecuencias por sus métodos. Si la guardaba, la cadena de custodia sería indefendible ante un tribunal.

La guardó en el bolsillo. Ya decidiría qué hacer con ella.

El móvil vibró de nuevo. No era Tomás.

Era un mensaje de un número desconocido. Seis palabras:

Bien jugado. Nos vemos en el próximo tablero.

Elena miró la pantalla durante un minuto entero. Luego, con un gesto que no era resignación ni desafío sino algo intermedio, guardó el móvil en el bolsillo y se quedó mirando por la ventana mientras Madrid despertaba bajo un cielo que no prometía nada.

FIN